Unit 3 Critical Thinking Questions

1. **In order to better protect yourself and your system, it is important to develop an understanding of various ways that hackers may attack your system. Choose two of the following attacks: DoS/DDoS, session hijacking, HTTP spoofing, DNS attacks, Backdoor attacks, man-in-the-middle (MITM) attacks, botnet attack. Explain what your two chosen attacks are and how they are used. Then find one newsworthy example of this attack in the news, citing your source.**

DDos (Denial of Service Attack) – Where a network is overloaded, causing it to not be available to its users. (Wikipedia DDos Attack)

Backdoor Attack – Where someone avoids normal authentication procedures to gain access to a system. (Backdoor Attack Warning Issued for WordPress Users)

2. **What is one specific example of the "cyber fingerprints" a hacker might leave behind after infiltrating a system? Provide and explain one reason a hacker might intentionally leave this identifying information.**

Hackers do this for the attention. The more complex and noticeable it is, the bigger it is going to be. An example of this is leaving a popup window with a note left for the user, with their "hacker name."

3. **Evaluate why there are still so many security holes in the internet, despite increased awareness of the importance of cybersecurity and the level of technological sophistication today. Are people or technology the real vulnerability in cybersecurity? Explain your answer by providing an example.**

The problem is that nothing can be made 100% secure. When new patches come out, people always find ways around them. Yes things can be more secure, but there is always another way to get around patches, as hard as we try to get rid of those backdoors. Both people and technology are the real vulnerability because the people are finding the problems in the technology to get through.

4. **Why is it important to apply patches quickly? How do some companies encourage quick application of patches (or how would you propose a company do so)? Do some exploring online if you need help coming up with a potential proposal for this.**

It is important because hackers work very quickly to find vulnerabilities in the patch. So by applying it quickly, you are beating them. Some companies will automatically update your computer through organization policies to get these patches on computers as quickly as possible.

5. **What is the first step a successful hacker is most likely to perform as part of their attack on a system? Include at least one description of what that step entails in practical terms/specific language.**

The first likely step they will take is reconnaissance. This is where the hacker engages with the system to figure out its vulnerabilities and backdoors, which will help them in their attack (to plan and execute it).